Homeland Security

July 18–22, 2011
Idaho Falls, Idaho

2011 Industrial Control Systems Advanced Cybersecurity Training

The United States Department of Homeland Security Control Systems Security Program is pleased to announce the July 2011 Industrial Control Systems (ICS) Cybersecurity Advanced Training.

This event will provide intensive hands-on training on protecting and securing industrial control systems from cyber attacks, including a Red Team/Blue Team exercise that will be conducted within an actual control systems environment. This exercise provides an opportunity to network and collaborate with other colleagues involved in operating and protecting control systems networks.

Where and When? July 18 – 22, 2011 at the Control Systems Analysis Center located in Idaho Falls, Idaho.

Who Should Attend? Members of the industrial control systems community associated with component and software development, IT and process control network operations and security, and operations/management of critical infrastructure assets and facilities.

Prerequisites: Each attendee should have practical knowledge with ICS networks, software, and components, have basic coding skills, and a fairly good understanding of IT network details such as the difference between UDP & TCP, and MAC & IP addresses. **Every student attending this course should bring a laptop computer** (with a DVD drive) that they have "administrator" privileges, allowing them to configure and load software.

Registration: Register at https://secure.inl.gov/icsadv0711/. The class size is limited to approximately 35 people, with a maximum of 2 individuals per company per event.

Structure and Agenda: This event includes 5 days of intensive cybersecurity for industrial control systems training, and a Red Team / Blue Team exercise:

Day 1 — Welcome, overview of the DHS Control Systems Security Program, a brief review of cybersecurity for Industrial Control Systems, a demonstration showing how a control system can be attacked from the internet, and hands-on classroom training on Network Discovery techniques and practices.

Day 2 — Hands-on classroom training on Network Discovery, using Metasploit, and separating into Red and Blue Teams.

Day 3 — Hands-on classroom training on Network Exploitation, Network Defense techniques and practices, and Red and Blue Team strategy meetings.

Day 4 — A 12-hour exercise where participants are either attacking (Red Team) or defending (Blue Team). The Blue Team is tasked with providing the cyber defense for a corporate environment, and with maintaining operations to a batch mixing plant, and an electrical distribution SCADA system.

Day 5 — Red Team/Blue Team exercise lessons learned and roundtable discussion.

For additional information and or questions send an email to: CSSP_Training@hq.dhs.gov